Terms used **encrypt circuit dummy** Found **52** of **185,942**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 52 Result page: **1** 2 3 next

Relevance scale

1 Security protocol for Frame Relay

Panagiotis Katsavos, Vijay Varadharajan
October 1993 **ACM SIGCOMM Computer Communication Review**, Volume 23 Issue 5
Publisher: ACM Press
Full text available: pdf(1.41 MB) Additional Information: full citation, abstract, index terms

This paper considers the protection of traffic using the Frame Relay service. First, we briefly describe the structure and functionality of the Frame Relay interface. Differences between the PTTs and the private vendor community with respect to Frame Relay interface are outlined. Then, we consider why the existing security protocols are inadequate in protecting the Frame Relay traffic effectively. This leads to the proposal of a new security sublayer (SFRC) which provides *Secure Frame Relay C ...*

2 Non-reversible VHDL source-source encryption

Kevin O'Brien, Serge Maginot
September 1994 **Proceedings of the conference on European design automation**
Publisher: IEEE Computer Society Press
Full text available: pdf(678.63 KB) Additional Information: full citation, references, index terms

3 Design and implementation of a scalable encryption processor with embedded variable DC/DC converter

James Goodman, Anantha Chandrakasan, Abram P. Dancy
June 1999 **Proceedings of the 36th ACM/IEEE conference on Design automation**
Publisher: ACM Press
Full text available: pdf(119.51 KB) Additional Information: full citation, references, citings, index terms

4 Masking the Energy Behavior of DES Encryption

H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(264.41 KB) Publisher Site Additional Information: full citation, abstract, index terms

Smart cards are vulnerable to both invasive and non-invasive attacks. Specifically, non-invasive attacks using power and timing measurements to extract the cryptographic key has drawn a lot of negative publicity for smart card usage. The power measurement techniques rely on the data-dependent energy behavior of the underlying system. Further, power analysis can be used to identify the specific portions of the program being executed to induce timing glitches that may in turn help to bypass key ch ...

5 A database encryption system with subkeys

George I. Davida, David L. Wells, John B. Kam
June 1981 **ACM Transactions on Database Systems (TODS)**, Volume 6 Issue 2
Publisher: ACM Press
Full text available: pdf(1.16 MB) Additional Information: full citation, abstract, references, citings, index terms

A new cryptosystem that is suitable for database encryption is presented. The system has the important property of having subkeys that allow the encryption and decryption of fields within a record. The system is based on the Chinese Remainder Theorem.

Keywords: data security, databases, decryption, encryption, subkeys

6 Security on FPGAs: State-of-the-art implementations and attacks

Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

7 Privacy-preserving credit checking

Keith Frikken, Mikhail Atallah, Chen Zhang
June 2005 **Proceedings of the 6th ACM conference on Electronic commerce**
Publisher: ACM Press
Full text available: pdf(166.37 KB) Additional Information: full citation, abstract, references, index terms

Typically, when a borrower (Bob) wishes to establish a tradeline (e.g., a mortgage, an automobile loan, or a credit card) with a lender (Linda), Bob is subjected to a credit check by Linda. The credit check is done by having Linda obtain financial information about Bob in the form of a credit report. Credit reports are maintained by Credit Report Agencies, and contain a large amount of private information about individuals. Furthermore, Linda's criteria for loan qualification are also private in ...

Keywords: e-commerce, privacy, secure multi-party computation, secure protocol

8 Design Method for Constant Power Consumption of Differential Logic Circuits

Kris Tiri, Ingrid Verbauwhede

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(146.44 KB) Additional Information: full citation, abstract, index terms

Side channel attacks are a major security concern for smart cards and other embedded devices. They analyze the variations on the power consumption to find the secret key of the encryption algorithm implemented within the security IC. To address this issue, logic gates that have a constant power dissipation independent of the input signals, are used in security ICs. This paper presents a design methodology to create fully connected differential pull down networks. Fully connected differential pul ...

9 Session 3A: markets and auctions II: Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions
Makoto Yokoo, Koutarou Suzuki
July 2002 **Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1**
Publisher: ACM Press
Full text available: pdf(181.62 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a secure dynamic programming protocol that utilizes homomorphic encryption. By using this method, multiple agents can solve a combinatorial optimization problem among them without leaking their private information. More specifically, in this method, multiple servers cooperatively perform dynamic programming procedures for solving a combinatorial optimization problem by using the private information sent from agents as inputs. Although the severs can compute the optimal soluti ...

Keywords: auction, dynamic programming, electronic commerce, privacy, public key encryption, security and agents

10 Routing: ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks
Jiejun Kong, Xiaoyan Hong
June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing**
Publisher: ACM Press
Full text available: pdf(236.79 KB) Additional Information: full citation, abstract, references, citings, index terms

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, AN ...

Keywords: anonymity, broadcast, mobile ad-hoc network, on-demand routing, pseudonymity, trapdoor, untraceability

11 Information flow: Private inference control
David Woodruff, Jessica Staddon
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(269.55 KB) Additional Information: full citation, abstract, references, index terms

Access control can be used to ensure that database queries pertaining to sensitive information are not answered. This is not enough to prevent users from learning sensitive information though, because users can combine non-sensitive information to discover something sensitive. Inference control prevents users from obtaining sensitive information via such "inference channels", however, existing inference control techniques are not private - that is, they require the server to learn what querie ...

Keywords: inference control, oblivious transfer, private information retrieval

12 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent
September 1977 **Proceedings of the fifth symposium on Data communications**
Publisher: ACM Press

Full text available: pdf(846.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

13 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach

Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(291.83 KB) Additional Information: full citation, abstract, index terms

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

14 Verification and security: Policy-hiding access control in open environment

Jiangtao Li, Ninghui Li
July 2005 **Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing PODC '05**
Publisher: ACM Press

Full text available: pdf(247.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In trust management and attribute-based access control systems, access control decisions are based on the attributes (rather than the identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's access control policy. In this paper, we develop a policy-hiding access control scheme that protects both sensitive attributes and sensitive policies. That is, Bob can decide whether Alice's certified attribute values satisfy Bob's policy, without Bob learning any ...

Keywords: access control, automated trust negotiation, cryptographic commitment, cryptographic protocol, digital credentials, evaluation, privacy, secure function

15 The development and proof of a formal specification for a multilevel secure system

Janice I. Glasgow, Glenn H. MacEwen
March 1987 **ACM Transactions on Computer Systems (TOCS)**, Volume 5 Issue 2
Publisher: ACM Press

Full text available: pdf(2.62 MB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper describes current work on the design and specification of a multilevel secure distributed system called SNet. It discusses security models in general, the various problems of information flows in SNet, and the abstract and concrete security model components for SNet. It also introduces Lucid as a language for specifying distributed systems. The model components are expressed in Lucid; these Lucid partial specifications are shown to be correct with respect to the formal model, and ...

16 Robust FPGA intellectual property protection through multiple small watermarks

John Lach, William H. Mangione-Smith, Miodrag Potkonjak
June 1999 **Proceedings of the 36th ACM/IEEE conference on Design automation**
Publisher: ACM Press
Full text available: pdf(119.08 KB) Additional Information: full citation, references, citings, index terms

Keywords: field programmable gate array (FPGA), intellectual property protection, watermarking

17 Designer's Workbench: Delivery of cad tools

R. A. Friendenson, J. R. Breiland, T. J. Thompson
January 1982 **Proceedings of the 19th conference on Design automation**
Publisher: IEEE Press

Full text available: pdf(666.88 KB) Additional Information: full citation, abstract, references, citings, index terms

Designer's Workbench (DWB) is a systematic approach to design aids integration that overcomes most of the barriers that frequently restrict the use of those aids. In combination with the UNIX* operating system [1,2], DWB manages both the flow and the form of data that is required by application programs that reside on various computer systems. The techniques described in this paper enable the Designer's Workbench development team to respond quickly to electrical and physical designers' need ...

18 Formal verification: Handling special constructs in symbolic simulation

Alfred Kölbi, James Kukula, Kurt Antreich, Robert Damiano
June 2002 **Proceedings of the 39th conference on Design automation**
Publisher: ACM Press
Full text available: pdf(109.20 KB) Additional Information: full citation, abstract, references, index terms

Symbolic simulation is a formal verification technique which combines the flexibility of conventional simulation with powerful symbolic methods. Some constructs, however, which are easy to handle in conventional simulation need special consideration in symbolic simulation. This paper discusses some special constructs that require unique treatment in symbolic simulation such as the symbolic representation of arrays, an efficient This paper discusses some special constructs that are unique to symb ...

Keywords: formal verification, symbolic simulation

19 Sensor networks (work in progress): Mobile traffic sensor network versus motion-MIX: tracing and protecting mobile wireless nodes

Jiejun Kong, Dapeng Wu, Xiaoyan Hong, Mario Gerla

November 2005 **Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks SASN '05**

Publisher: ACM Press

Full text available: pdf(374.84 KB) Additional Information: full citation, abstract, references, index terms

In this paper we focus on passive attacks that threaten the privacy of mobile wireless networks. We define the concept of "venue privacy attack" (VPA) to illustrate the emerging anonymity attacks to trace mobile wireless nodes. Then we propose "motion-MIX" as the countermeasure to defend against various venue privacy attacks. We study the necessary conditions to implement motion-MIXes. These conditions include identity-free routing, one-time packet content and various other concerns in the netwo ...

Keywords: ANODR, anonymity, identity-free routing, mobility, motion-MIX

20 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2

Publisher: ACM Press

Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

Results 1 - 20 of 52 Result page: **1** 2 3 next

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4199	((326/8) or (703/13) or (703/15) or (713/187) or (713/190) or (716/4)).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/10/03 12:10
L2	7086119	1 an d(@pd > "20060609")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:11
L3	305	1 and (@pd > "20060609")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:31
L4	6588	(scrambl$3 encrypt$3) near4 circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:32
L5	4731	(scrambl$3 encrypt$3) near2 circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:32
L6	113	(scrambl$3 encrypt$3) near2 circuit same (dummy decoy false redundant)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:40
L7	13	((scrambl$3 encrypt$3) near2 circuit same (dummy decoy false redundant)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:43
L8	1043	(713/189).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/10/03 12:43
L9	176	8 and (encrypt$3 scrambl$3) with circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:43

EAST Search History

S1	1	("20020083330").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/10 13:16
S2	16	dummy adj circuit with (combin$3 encrypt$3 scrambl$3 encipher$4 encod$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:53
S3	126	code adj obfuscat$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:57
S4	2727	((326/8) or (703/13) or (703/15) or (713/187) or (713/190) or (716/4)). CCLS.	USPAT	OR	OFF	2006/10/03 12:10
S5	289	S4 and (@pd > "20051117")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:58
S7	1	("5748741").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/09 14:03
S8	1	("6088452").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/09 14:03